Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7


SUBJECT: Guidelines Covering Disclosure of Classified Intelligence

CONCURRENCE:

(Signed) Thomas E. Parrott for

Bronson Tweedy
Deputy to the DCI
for National Intelligence
Programs Evaluation

26 Oct 71
Date

25X1

[redacted]

Edward W. Proctor
Deputy Director
for Intelligence

27 OCT 1971
Date

Thomas H. Karamessines

Thomas H. Karamessines
Deputy Director for Plans

1971
Date

25X1

[redacted]

Carl F. Duckett
Deputy Director
for Science & Technology

Date

25X1

[redacted]

John W. Coffey
Deputy Director
for Support

Date


Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

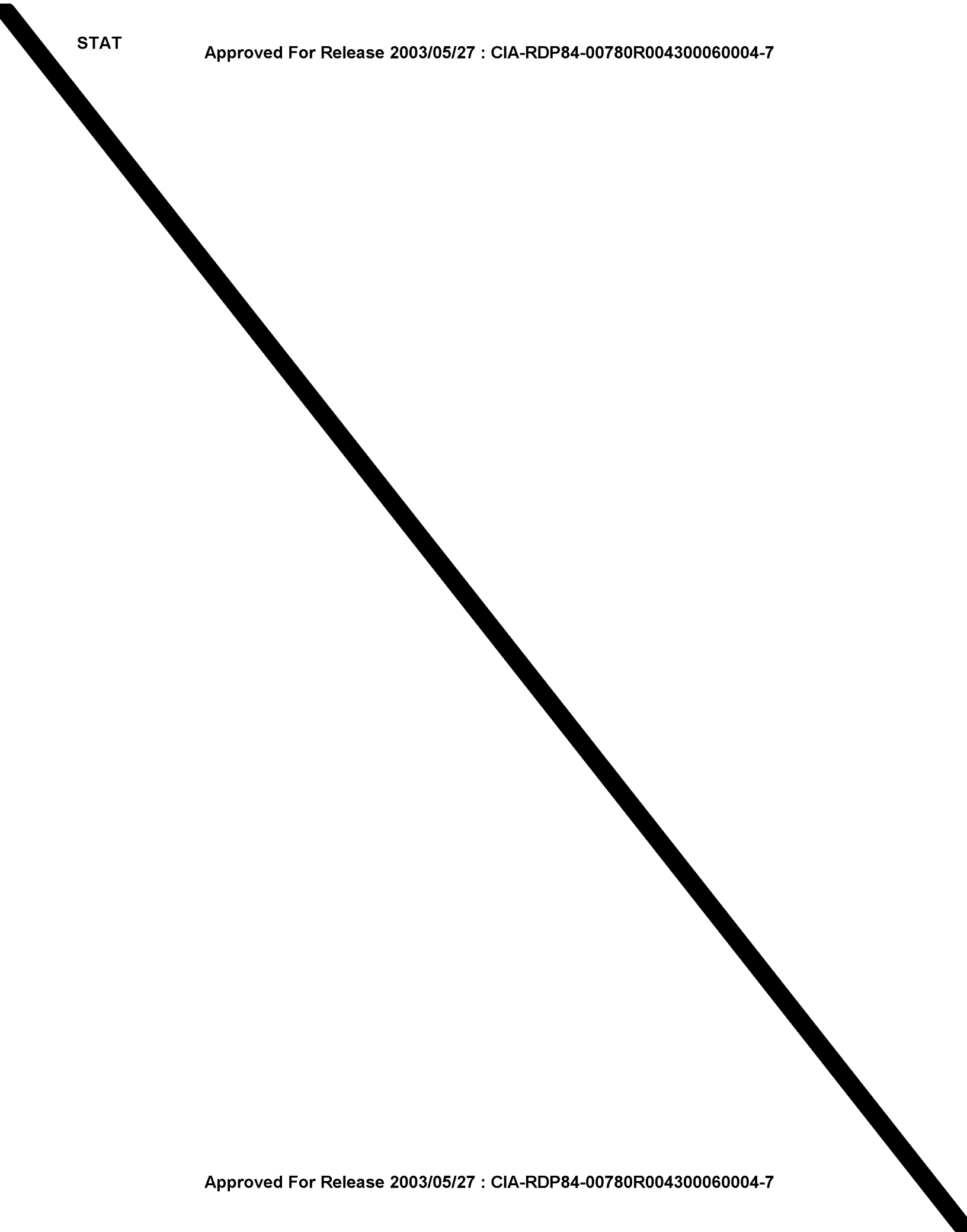

SUBJECT: Guidelines Governing Disclosure of Classified Intelligence

Distribution:
Orig - Return to OS
1 - DDCI
1 - ER
1 - D/NIPE
1 - DD/I
1 - DD/P
1 - DD/S&T
2 - DD/S

ILLEGIB


Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

STAT
Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7



Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

7/4/47

SECRET

4 NOV 1971

MEMORANDUM FOR: Chairman, United States Intelligence Board

SUBJECT : Guidelines Governing Disclosure of Classified Intelligence

1. On 21 December 1970, the President in noting your statutory responsibilities for the protection of intelligence sources and methods, instructed that guidance be provided in this field especially through the machinery of the intelligence community.

2. On 23 April 1971 such guidance was promulgated to the intelligence community within the framework of the United States Intelligence Board through USIB-D-9.2/39, entitled, "Guidance Governing Disclosure of Classified Intelligence."

3. In a companion report to the President you advised that periodic reports would be requested from the Board Principals on those measures taken within their respective agencies and departments to implement these guidelines.

4. On 7 October 1971 you requested the Board Principals to report by the end of October or early November on the measures taken in this regard within their respective agencies or departments.

5. The following sets forth the Subject guidelines and the appropriate response of the Agency to comply with them.

Guideline No. 1

Review existing departmental and agency regulations governing the control of classified information to make sure that in every instance they meet the criteria required by the steadily



GROUP 1
Excluded from automatic downgrading and declassification

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

increasing volume and significance of classified intelligence, particularly including sensitive compartmented intelligence. Particular emphasis should be placed on assuring that the need-to-know principle is strictly enforced.

Response:

1) During the past three years, fifteen regulations in the Security series have been revised, or are under revision. These regulations, as a matter of policy, are continuously reviewed and amended when necessary.

2) These Central Intelligence Agency regulations and procedures assure that only those individuals with a demonstrated "need-to-know" receive classified information and that all recipients are constantly aware of the necessity to protect it from public disclosure.

3) A recent Security Clearance Review conducted by the Agency, utilizing a strict "need-to-know" criteria, resulted in the cancellation of [redacted] Codeword clearances held by Agency employees. In addition, [redacted] Top Secret and/or Codeword clearances granted by CIA and held by the employees of private business, or consultants were also cancelled.

25X9

25X9

4) Every six months each Agency employee must attest by signature that he or she has again read the Agency Handbook entitled, "Employee Conduct and Discipline." These rules of conduct delineate employee responsibilities both on and off the job, including an explanation of the "need-to-know" principle.

5) There has been established within CIA a panel, which among its requirements, has been tasked to review Agency Security



Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

Compartmentation relating to: (a) personnel access to Compartmented information, (b) document controls, (c) information dissemination, (d) physical security, (e) communications, and (f) sanitising classified data, including declassification and downgrading procedures.

25X1 (6) Compartmented "Control" and [redacted] Security Officers are designated within the Agency to assure that only those individuals who have a strict "need-to-know" are granted access to Codeword and Compartmented information and/or materials. After such "need-to-know" has been clearly demonstrated, appropriate briefings are given regarding the system, and later upon termination from the system, pertinent debriefings are likewise effected. These Compartmented and Codeword procedures are set forth in Agency Manuals originated specifically for setting forth guidelines and procedures governing these special systems.

(7) An Agency Task Force recently completed a survey to reduce vulnerabilities of classified information stored in non-CIA facilities. The survey reflected that there are [redacted] in which CIA classified data is stored. Whenever classified information is found to be stored in a facility which does not meet minimum standards for secure storage, the Director of Security will advise the appropriate Deputy Director or Head of Independent Office and require that continued storage be justified by operational necessity. Thereafter, the Office of Security will undertake a follow-up program to ensure compliance with its recommendation to achieve effective physical security at the earliest possible 25X1



Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

date and will develop a schedule to resurvey every two years, all facilities where classified data is stored.

(8) Since August 1968, on a selective basis, the Agency has provided special security briefings to its personnel in order to improve the protection of classified information in those components of CIA which reflect a greater need based upon statistical figures involving personnel charged with security violations. The Special Briefing Program has achieved notable results ranging from 33 per cent to 58 per cent improvement in the offices concerned and a 10 per cent overall drop in security violations throughout the Agency.

Guideline No. 2

Make sure that briefing and indoctrination procedures are reviewed with the objectives of Guideline No. 1 above in view. These procedures should be so designed as to assure that newly indoctrinated members of the intelligence community and other newly indoctrinated officials of the Government fully understand the differences which exist among various kinds of intelligence, with respect to danger to the source or method which would result from disclosure. It should also be the purpose of these procedures to explain the way in which cleared individuals can readily ascertain the clearance status of others before discussing classified information revealing intelligence sources and methods, and to make sure that they do so.

Response:

(1) Agency briefing and indoctrination procedures are reviewed continuously to meet the changing times. All persons entering on duty receive eight hours of security education covering such matters as security regulations, espionage threats to CIA and the intelligence community, protection of sources, methods and


Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

techniques of intelligence, unauthorized disclosures, physical and technical penetrations, outside activities, security assistance to all employees and physical security.

(2) Employees returning from overseas are given security briefings in conjunction with the CIA Review Program. These briefings bring the employees up-to-date on the latest security practices which originated while they were abroad.

(3) Agency employees are given comprehensive security briefings when travelling to denied areas. They are also briefed on security matters when scheduled for TDY, PCS and private travel outside the United States.

Guideline No. 3

Provide for periodic reindoctrination and continuing education in special security practices and procedures relating to intelligence, in addition to those security procedures established as general policy, to include a program for prompt debriefing of individuals who no longer have a need-to-know.

Response:

(1) A Reindoctrination Program for all Agency employees is given periodically and new security approaches and procedures are constantly explored to form the basis of the next program which always includes an updating of the last one.

(2) The Agency has an effective program for the prompt debriefing of individuals who no longer have a need-to-know in the various categories of clearance, including Compartmented information.



Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

Guideline No. 4

Review procedures for authorizing and controlling disclosures and releases.

a. The responsibility of the intelligence chief for assessing the risk to intelligence sources and methods involved in deliberate disclosures should be delineated. There should be a review and assessment by intelligence authorities whenever any classified intelligence is proposed for declassification or for use in briefings, testimony, symposiums, seminars, speeches, writings for publication, presentations, courses of instruction, press releases, formal and informal interviews with press representatives, or other activities in the course of which there is a danger that intelligence sources and methods might be revealed.

Each assessment should include methods by which such intelligence can be effectively and plausibly sanitized by or with the approval of the originating agency so as to protect the source. Sensitive intelligence to be disclosed should be clearly identified as such and the official disclosing it should be so cautioned when appropriate. This can be particularly important in dealing with some public information officials who cannot be expected to be fully familiar with the origins of such sensitive intelligence. Records should be maintained regarding any classified intelligence declassified or authorized for disclosure.

Response:

It is the policy of the Agency not to make deliberate disclosure of classified intelligence information to the public. In order to prevent the unauthorized release of such data CIA procedures and regulations as outlined in Headquarters



Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

Regulation [ ] require employees to submit their writings, or the subject matter of public speeches to their respective Deputy Directors or Heads of Independent Offices for their review and the subsequent approval of the Director of Security.

25X1

Guideline No. 4 continued

b. The facts surrounding inadvertent disclosure of classified intelligence to any person or persons not authorized for access to such intelligence should be reported to the appropriate intelligence chief, who will inform the originating agency in any potentially harmful case.

c. Any person having knowledge of any disclosure of classified intelligence made contrary to the regulations and controls of the department or agency concerned should promptly report it to the appropriate intelligence chief for action. Such action may include (1) such steps as are feasible to repair or limit the extent of the damage; (2) a request for investigation by appropriate authorities; (3) an assessment of the possible harm to intelligence sources and methods and notification to all intelligence authorities concerned; and (4) prompt notification to all official recipients that an unauthorized disclosure has occurred, together with advice of remedial action to be taken and guidance for responses to inquiries from public media representatives that may result from the compromise.

Response:

(1) The Security Committee of the United States Intelligence Board was established to promote means by which the intelligence

STATINTL

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

community may prevent the unauthorized disclosure of intelligence, intelligence information and intelligence sources and methods. Characteristic of the Security Committee response is prompt inquiry into the facts surrounding serious unauthorized disclosures and consultation with the appropriate intelligence agencies represented on the Committee. The scope and seriousness of the disclosure is analyzed by the participating agencies and departments most affected and concerned with the "leak" of classified information. Determinations are made in these cases of significance as to the feasibility of investigation. Paramount consideration is given to the time frame of the disclosure and the extent of the source material dissemination within the intelligence community since these factors have a salient bearing on the fruitfulness of investigative inquiry.

(2) A centralized data base covering leaks of intelligence information to public information media has been established in the Office of Security. It contains a copy of the news media article, its author, the name of the publication in which it appeared, the gravity of the leak, and where appropriate, an assessment of the damage.

Guideline No. 5

Take fully into account, in proposing the release of any intelligence derived from a joint project in the intelligence community, the interests of any other members of the intelligence community which might be concerned. If a department or agency authorizes the disclosure of sensitive intelligence from such a



Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7


community may prevent the unauthorized disclosure of intelligence, intelligence information and intelligence sources and methods. Characteristic of the Security Committee response is prompt inquiry into the facts surrounding serious unauthorized disclosures and consultation with the appropriate intelligence agencies represented on the Committee. The scope and seriousness of the disclosure is analyzed by the participating agencies and departments most affected and concerned with the "leak" of classified information. Determinations are made in those cases of significance as to the feasibility of investigation. Paramount consideration is given to the time frame of the disclosure and the extent of the source material dissemination within the intelligence community since these factors have a salient bearing on the fruitfulness of investigative inquiry.

(2) A proposal to establish a centralized data base in the Office of Security covering unauthorized disclosures of classified information is in the process of coordination. Information covering the nature and author of the leak, the name of publication in which it appears, the gravity of the leak, and any information which might reveal the source of the leak will be filed in the proposed centralized data base.

Guideline No. 5

Take fully into account, in proposing the release of any intelligence derived from a joint project in the intelligence community, the interests of any other members of the intelligence community which might be concerned. If a department or agency authorizes the disclosure of sensitive intelligence from such a



Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7
SECRET

source, that agency is responsible for informing other USIB members of the action. Special attention should be given to defining the precise limits of the disclosure and the cautioning against inadvertent elaboration or extension beyond those limits.

Response:

The restriction on dissemination of classified information is commonly known as the Third Agency Rule. Director of Central Intelligence Directive No. 1/7, "Controls for Dissemination and Use of Intelligence and Intelligence Information" reinforces the application of the Third Agency Rule which was agreed to by the member agencies of USIB. Agency Regulation [redacted] also clearly sets forth the policy application of the Third Agency Rule. It states that classified or controlled intelligence information originating in another department or agency shall not be disseminated or used outside of CIA without permission of the originating department or agency except under certain conditions. These conditions permit dissemination when: (1) the document is originated by a USIB member agency or department and the document contains no limiting control marking and (2) USIB member agencies have given advance consent for the dissemination of finished intelligence to USIB members providing the document does not bear any control markings and the data is paraphrased to conceal the originating agency, the source, the place and date acquired and the manner of acquisition.

25X1



SECRET
Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7


**Guideline No. 6**

**In conjunction with appropriate authority, take, or assure that disciplinary action is taken where appropriate, in a just, clear, and definite manner which will demonstrate the extreme seriousness with which unauthorized disclosures are viewed. Where a violation of criminal statutes may be involved, any such case should be referred promptly to the Department of Justice.**

**Response:**

**(1) Headquarters Regulation** [redacted] 25X1
**prohibits all Agency employees from using official data for any purpose other than the performance of their official duties for use on behalf of the Agency. Further each employee is charged with the responsibility for the secure handling of official data and for protecting it against unauthorized disclosure.**

**(2) Headquarters Regulation** [redacted] 25X1
**sets forth the penalties incurred for failure to use official data properly or to protect it from unauthorized disclosure. These penalties range from an oral reprimand by a division chief or higher authority to termination, depending upon the circumstances and gravity of the offense.**

**(3) As recently as 10 June 1971 the Deputy Director for Support through Headquarters Notice** [redacted] **advised all CIA** 25X1
**employees of the President's concern over disclosures in the public media of classified information bearing upon important aspects of national security, particularly those disclosures that may**




Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7


jeopardize intelligence sources and methods. The Notice identified the Assistant to the Director of Central Intelligence as the responsible authority for the coordination within the Agency of responses to inquiries from representatives of public information media and stated that the Director was prepared to take strong disciplinary action against any employee who jeopardized intelligence sources and methods through unauthorized disclosure.

/S/

R. E. Cushman, Jr.
Lieutenant General, USMC
CIA Member of USIB


Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7

SUBJECT: Guidelines Governing Disclosure of Classified Intelligence

ORIGINATOR:

25X1

[redacted]

Howard W. Osborn
Director of Security

26 OCT 1971
Date

Distribution:
Orig - Addressee
1 - DDCI
1 - ER
1 - D/NIPE
1 - DD/I
1 - DD/P
1 - DD/S&T
2 - DD/S
1 - D/Security

Approved For Release 2003/05/27 : CIA-RDP84-00780R004300060004-7